

RECEIVED
CENTRAL FAX CENTER

APR 10 2007

REMARKS

Reconsideration of the application is requested.

Claims 1-21 remain in the application. Claims 1-21 are subject to examination.

Under the heading "Claim Rejections - 35 USC § 102" on pages 2-5 of the above-identified Office Action, claims 1-6, 13-16 and 21 have been rejected as being fully anticipated by U.S. Patent No. 5,757,918 to Hopkins (hereinafter Hopkins) under 35 U.S.C. § 102.

Applicant lays out an in-depth analysis of the Hopkins reference for the Examiner's reconsideration. Hopkins teaches a smart card 12 and a verifier 24, 50. First, the smart card has the following preloaded information:

U - Public identification of user;

e - Public key exponent;

n - Public key modulus; and

$E_p[aB]$ - "Encrypted aB" - a & B are secret values, a depends on private public key d, U and n and pin P. B depends on U, n, P and d (see column 2, lines 56-67).

The verifying unit or terminal 24, 50 is preloaded with:

e - Public key exponent; and
n - Public key modulus (see Fig. 2).

Second, the smart card 12 is inserted in a reading device (the terminal 24). The user is requested to enter pin p via a keypad of the terminal 24, 50. The pin value P is used to decrypt $E_p[aB]$ (encrypted aB) resulting in aB. The value a is now determined from $a \equiv P(UP)^d \text{ mod } n$. The value B is determined as shown in column 5.

Third, the smart card 12 generates a random number x and computes the value:

$$T = x^e \text{ (mod } n \text{)}.$$

The value T is transmitted to the terminal 24 along with the value U (see column 3, lines 19-24 and Fig. 3). As values e and n are known to both the smart card 12 and the verifier 24, 50 it is public keying material and T is a process of symmetrical authentication as public keys are used for the encryption.

Fourth, the terminal 24 then generates a random number y, being a challenge number, and sends the random number y to the smart card 12.

Fifth, the smart card 12 generates a response value S . S is a function of y , x , aB , and n . $S = x(aB)^y \pmod n$ (see column 6, lines 22-26). S is transmitted back to the terminal 24 (column 3, lines 27-31). As aB is only known to the smart card it is private keying information. Therefore S is returned as a digital signature (asymmetric authentication) and requires a high amount of computational effort.

Sixth, the terminal 24 then computes a value T' which is a function of y , n , S , e and U . $T' = S^e U^y \pmod n = x^e \pmod n$.

Seventh, T' is compared to T in the terminal 24. If a match is found, the card is verified.

Eighth, the terminal 24 may communicate with a host 14 of a secure facility 20. All communications between the host 14 and the terminal 24 is encrypted (see column 4, lines 36-48).

Turning now to the invention of the instant application. In steps b) - e) an asymmetric algorithm is used. The verifying unit generates a data element 9 (step b) and encrypts it using a public key of the proving unit (step c) before sending it to the proving unit (step d). The encrypted data element 9 can only be decrypted by using a private key of the proving unit and is therefore secret or asymmetric (step e). After the decryption of the encrypted data element in step e) the data

element is known to both the verifying unit and the proving unit. It is therefore a shared secret key, which is used in steps f) to i) as a key to authenticate the data set by a challenge and response method. Before discussing steps f) - i), it is important to note that the private key in the instant application is only used for decryption and not for forming a digital signature which is computationally intensive. This is in contrast with Hopkins which uses the private key aB for forming a computationally intensive digital signature in the formulation of the value S as noted above. In addition, the formulation of S is not a decryption it is an encryption and very computationally intensive.

Step e) of the instant application recites:

using the proving unit to decrypt the encrypted data element in a first decryption method, assigned to the first cryptographic encryption method, using a private key known only to the proving unit (emphasis added).

The Examiner states that step e) is read on by Hopkins and refers to column 3, lines 27-28 of Hopkins which teaches that the smart card decrypts $E_p[aB]$ using the pin P. This analysis is respectfully stated to be improper for two reasons. First, the value $E_p[aB]$ resides permanently in memory of the smart card in Hopkins. In Hopkins, the value $E_p[aB]$ is not first formulated and encrypted on the terminal 24 and sent to the smart card 12 to be decrypted rather it is always on the smart card. In contrast, in the invention of the instant

application, this is what happens in steps b) - d) of claim 1. Second, the pin P is not a private key. By definition a private key can only be known and permanently stored in the smart card and is never transmitted to the smart card where it can be intercepted. The use of a private key provides a much higher level of security than a pin (see page 2, lines 7-21 of the instant application contrasting a private key and a pin number). In Hopkins the private key is aB. The value aB is used for encryption to form the value S. As noted this requires significant computational processing. In other words, the private key aB of Hopkins is not used for decryption purposes by the smart card itself.

Steps f) to h) of claim 1 of the instant application teach a symmetrical encryption algorithm using the common public key.

The Examiner states that step f) of the instant application is read on by column 3, lines 25-30 of Hopkins. Step f) of claim 1 recites calculating an authenticator 11 from the data set and the data element. Hopkins teaches that the smart card formulates a value T derived from a random number x generated on the smart card and public keys e and n. Further Hopkins teaches the encryption of the data set y provided from the terminal. Certainly Hopkins teaches encryptions of the data set x or y by the smart card and the encrypted data set is sent to the terminal 24. However, the data set x is not

encrypted in dependence on a data element sent from the terminal 24 and cannot read on step f) as the authenticator 11 is encrypted by the data element 9, functioning as a second public key, which is not generated on the smart card but on the terminal in the instant application. Second, the data set y of Hopkins does indeed meet the criteria of being sent from the terminal 24. However, the data set y is encrypted via the private key aB and not from the second public key (the data element) first sent from the terminal, decrypted and then used for encrypting the data set.

In other words, in the instant application, a data element is generated and first public key encrypted in the terminal 2, sent to the smart card 1, decrypted using a private - public key pair resulting in the data element. The data element now functions as a second public key for encryption of the data set. Simply put, in Hopkins no data element is sent from the terminal 24, 50 to the smart card 12 which functions as a second public key for encrypting purposes. In Hopkins the public key elements e, n are both known initially in both the smart card and the terminal. No "second public key" is formulated in Hopkins and used for encryption purposes.

In regards to step c) of claim 1, the Examiner cites column 4, lines 39-40 of Hopkins. However, the context of the cited lines refers to the communication of the remote facility 22

with the secure facility 20 over the network communications link 26, as shown in Fig. 1 (see column 4, lines 34 - 43). This is not communications between the prover or smart card and the terminal and therefore Applicant does not understand what the Examiner wishes to teach from this section of Hopkins.

In summary, the Examiner is requested to cite in Hopkins where:

- a) a private key is used for decryption in the smart card; and
- b) a second public key (data element) is formulated and encrypted in the terminal, sent to the smart, decrypted with a private key, and used for encrypting data sent back to the terminal. Simply put, this is not taught in Hopkins.

Under the heading "Claim Rejections - 35 USC § 103" on pages 6-10 of the above-identified Office Action, claims 7-12 and 17-20 have been rejected as being obvious over Hopkins in view of U.S. Patent No. 5,272,755 to Miyaji et al. (hereinafter Miyaji) under 35 U.S.C. § 103.

Claims 7-12 and 17-20 ultimately depend on claim 1. Because claim 1 is believed to be allowable, claims 7-12 and 17-20 are also believed to be allowable.

RECEIVED
CENTRAL FAX CENTER

APR 10 2007

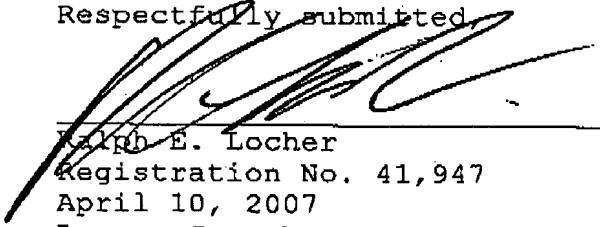
It is accordingly believed to be clear that none of the references, whether taken alone or in any combination, either show or suggest the features of claim 1. Claim 1 is, therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claim 1.

In view of the foregoing, reconsideration and allowance of claims 1-21 are solicited.

If an extension of time is required, petition for extension is herewith made. Any extension fee associated therewith should be charged to the Deposit Account of Lerner Greenberg Stemer, LLP, No. 12-1099.

Please charge any other fees that might be due with respect to Sections 1.16 and 1.17 to the Deposit Account of Lerner Greenberg Stemer LLP, No. 12-1099.

Respectfully submitted



Ralph E. Locher
Registration No. 41,947
April 10, 2007
Lerner Greenberg Stemer LLP
P.O. Box 2480
Hollywood, Florida 33022-2480
Tel.: (954) 925-1100 Fax: (954) 925-1101

- Page 9 of 9 -